

УТВЕРЖДАЮ



/ В.В. Баранов /

« 27 » июня 2024г.

**ЗАДАНИЕ НА ПРОЕКТИРОВАНИЕ**

**«МОДЕРНИЗАЦИЯ СИСТЕМ ОХРАННОГО ВИДЕОНАБЛЮДЕНИЯ»**

Объект: Гатчинское отделение по сбыту электроэнергии

АО «Петербургская сбытовая компания»

## ОГЛАВЛЕНИЕ

1	НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ.....	3
1.1	НАЗНАЧЕНИЕ СИСТЕМЫ.....	3
1.2	ЦЕЛЬ СОЗДАНИЯ СИСТЕМЫ.....	3
2	ХАРАКТЕРИСТИКИ ОБЪЕКТА .....	3
3	ТРЕБОВАНИЯ К СИСТЕМЕ .....	3
3.1	ТРЕБОВАНИЯ К СТРУКТУРЕ И ФУНКЦИОНИРОВАНИЮ СИСТЕМЫ .....	3
3.1.1	КОМПОНЕНТЫ СИСТЕМЫ.....	3
3.1.2	ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ.....	4
3.1.3	ТРЕБОВАНИЯ К БАЗЕ ДАННЫХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ .....	6
3.1.4	ТРЕБОВАНИЯ К ИНТЕГРАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.....	7
3.1.5	ТРЕБОВАНИЯ К ИНТЕРАКТИВНОЙ КАРТЕ .....	7
3.1.6	ТРЕБОВАНИЯ К ПРОТОКОЛИРОВАНИЮ СОБЫТИЙ .....	9
3.1.7	ТРЕБОВАНИЯ К УДАЛЁННЫМ РАБОЧИМ МЕСТАМ.....	9
3.1.8	ТРЕБОВАНИЯ К СПОСОБАМ И СРЕДСТВАМ СВЯЗИ МЕЖДУ КОМПОНЕНТАМИ СИСТЕМЫ .....	10
3.1.9	ТРЕБОВАНИЯ К СОВМЕСТИМОСТИ С ДРУГИМИ СИСТЕМАМИ .....	11
3.1.10	ТРЕБОВАНИЯ К РЕЖИМАМ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ.....	11
3.1.11	ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ.....	11
3.2	ТРЕБОВАНИЯ К ЧИСЛЕННОСТИ ПЕРСОНАЛА .....	11
3.3	ПОКАЗАТЕЛИ НАЗНАЧЕНИЯ .....	12
3.4	ТРЕБОВАНИЯ К НАДЁЖНОСТИ .....	12
3.5	ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ.....	13
3.6	ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ .....	13
4	СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ.....	14
5	ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ .....	15
6	ИСТОЧНИКИ РАЗРАБОТКИ.....	16
7	ОСОБЫЕ УСЛОВИЯ .....	16
ПРИЛОЖЕНИЕ 1 .....		<b>ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.</b>

## **1 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ**

### **1.1 НАЗНАЧЕНИЕ СИСТЕМЫ**

Система охранного видеонаблюдения (СОВ) предназначена для круглосуточного мониторинга и видеорегистрации на территории и в помещениях защищаемого объекта, а также предоставления видеоинформации и аналитики.

### **1.2 ЦЕЛЬ СОЗДАНИЯ СИСТЕМЫ**

Основной целью модернизации системы охранного видеонаблюдения является приведение характеристик существующей системы к современному техническому уровню для решения задач по защите людей от возможных попыток террористических угроз, защите от возможных попыток хищения имущества, а также предотвращению несанкционированного доступа на территорию объекта, проведения служебных расследований в части произошедших инцидентов, в том числе предоставление видеоинформации об инциденте по запросам органов власти.

## **2 ХАРАКТЕРИСТИКИ ОБЪЕКТА**

Объект представляет собой клиентский офис АО «Петербургская Сбытовая Компания», находящийся по адресу: Ленинградская область, г. Гатчина, ул. Старая дорога, д.2, Гатчинское ОСЭ. Объект представляет из себя двухэтажное кирпичное здание капитальной постройки зданий общей площадью 490,2 кв. метров с прилегающей закрытой охраняемой территорией, на которую можно проникнуть через въездные ворота.

## **3 ТРЕБОВАНИЯ К СИСТЕМЕ**

### **3.1 ТРЕБОВАНИЯ К СТРУКТУРЕ И ФУНКЦИОНИРОВАНИЮ СИСТЕМЫ**

#### **3.1.1 КОМПОНЕНТЫ СИСТЕМЫ**

СОВ должна состоять из:

- Внешних стационарных IP-видеокамер охраны периметра не ниже 2Мр, передающих видео с разрешением Full HD со скоростью 30 кадров/с., оснащенных моторизированным объективом с фокусным расстоянием  $f=2,8-12\text{мм}$  и инфракрасной подсветкой (дальностью 30м), расположенных на стенах здания на расстоянии 20 – 50 м друг относительно друга, обеспечивающих непрерывное наблюдение за зоной, непосредственно прилегающей к зданию с внешней и внутренней сторон шириной не менее 10 м, общим количеством не менее 7 ед. Российское производство.
- Внутренних 2Мр купольных IP-видеокамер, передающих видео с разрешением Full HD со скоростью 30 кадров/с. с варифокальными объективом с фокусным расстоянием  $f=2,8-12\text{мм}$  и инфракрасной подсветкой (дальностью 30м), что позволяет получать качественное видео на плохо освещенных участках. IP-камера работает в двух режимах – DirectIP и ONVIF, в каждом режиме есть возможность настройки нескольких независимых потоков и использование разных потоков на запись и мониторинг. Низкое энергопотребление возможно за счет питания по PoE. Предусмотрена интеграция IP-видеокамеры с охранными системами, используя тревожный вход/выход общим количеством не менее 5 ед. Российское производство.
- Встроенная аналитика:
  - Обнаружение движения с настройкой чувствительности для дневного и ночного времени суток и размеров объекта.
  - Пересечение зоны контроля как во внутрь, наружу, так и в обоих направлениях.
  - Взлом или саботаж — обнаружение факта расфокусировки объектива, изменения положения объектива, заслон посторонними предметами.

- Поддерживается работа с тревожными входами, а также контроль состояния системы и microSD карты.
- Обработка всех событий возможна по следующим сценариям:
  - Активацией релейного выхода.
  - Отправка извещения по email.
  - Дистанционный вызов в программное обеспечение.
  - Отправка изображений на FTP сервер.
  - Запись события на microSD карту.
- Специализированного программного обеспечения, реализующего автоматические и полуавтоматические сценарии реакции на события, широкие функции самодиагностики и видеоаналитики (детектора движения (основной, инфракрасный и с выбором направления); детектора лиц; детекторов расфокусировки, засветки, стабильности видеосигнала, изменения фона видеоизображения, закрытия объектива видеокамеры); настройки, администрирования, управления и мониторинга системы; функции оповещения, просмотра видео с использованием веб-сервера, RTSP-сервера.
- Специализированного серверного оборудования, обеспечивающего высококачественную запись (HD) и надежное хранение видеоизображений в течение не менее 30 суток, с функциями администрирования, самодиагностики, резервного копирования, размещенного в помещении серверной. Предусмотреть возможность оперативного восстановления конфигурации системы к последним настройкам управляющего ПО СОВ.
- Одна рабочая станция мониторинга, оснащенных FullHD-монитором с размером диагонали не менее 30", обеспечивающей возможность отображения не менее 16-ти камер, размещенная на посту охраны.
- Оборудованием гарантированного электропитания на базе ИБП с резервными аккумуляторными блоками, обеспечивающим непрерывную работу серверного оборудования и рабочих станций на протяжении не менее 30 минут. В серверных/кроссовых помещениях применять ИБП двойного преобразование, платы сетевого управления и мониторинга.
- Сеть передачи данных и гарантированного электропитания должна состоять из:
  - Коммуникационного, коммутационного и линейно-кабельного оборудования, обеспечивающего надежное резервируемое подключение элементов систем между собой, функционирование систем и элементов в круглосуточном режиме. Источников бесперебойного питания (ИБП) с аккумуляторными батареями (АКБ), обеспечивающими функционирование СОВ в случае пропадания электропитания в течение не менее 30 минут.
- Система должна предусматривать возможность организации отдельных рабочих мест для администрирования системы, а также нескольких рабочих мест операторов системы (количество согласовывается с Заказчиком).

### 3.1.2 ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ.

ПО СОВ должно иметь клиент-серверную архитектуру. На объекте должна быть обеспечена взаимоувязанная, интегрированная работа всех систем обеспечения безопасности (СКУД, СОВ, и др. (охранная сигнализация, пожарная сигнализация - по отдельному заданию).

ПО СОВ должно обеспечивать:

- Визуализация информации и управления системами на основе единого интерфейса;
- Использование многоуровневой интерактивной карты подконтрольного объекта, обеспечивающей реализацию следующих функций: автопереключение и рекурсивный поиск



связей на карте; использование на карте активных символов устройств с возможностью управления устройствами из контекстного функционального меню;

- Автоматизация верификации тревожных событий и организации реагирования на происшествия, учет, систематизация, подготовка отчетов по выявленным событиям, функционированию систем;
- Обеспечение резервирования основных критических элементов систем, применение средств и инструментов мониторинга работоспособности и самодиагностики основных элементов систем с отображением их состояния на общей структурной схеме.
- Удаленное взаимодействие центральных компонентов подсистем СОВ и СКУД и автоматическая репликация внутренних баз данных (содержащих параметры настройки систем и данные о зарегистрированных в системах событиях);
- Платформа безопасности должна быть распределенной;
- Платформа должна быть открытой для внешней интеграции с использованием SDK позволяющим полностью управлять всеми элементами подсистемы, получать события и отсылать команды (реакции);
- Возможность централизованной регистрации и обработки событий, поступающих от подсистем, генерация оповещений и управляющих воздействий в соответствии с гибко настраиваемыми алгоритмами реакций подсистем, так называемая событийная модель управления;
- Неограниченные возможности масштабирования, адаптации к специфике решаемых задач, перераспределения используемых ресурсов при изменении количества или качества задач по мониторингу состояния подконтрольных объектов и управления различного рода оборудованием, возможность маршрутизировать события внутри системы;
- Возможность использования внутри одной системы безопасности различных типов сетевых соединений: LAN, Internet, Modem, WiFi и т.д. с разной скоростью передачи данных;
- Удаленное взаимодействие центральных компонентов подсистемы и автоматическую репликацию внутренних баз данных (содержащих параметры настройки системы и данные о зарегистрированных в системе событиях), входящих в состав ИСБ;
- Программный и аппаратный контроль работоспособности центральных компонентов системы;
- Возможность формирования любых отчетов по событиям;
- Автоматические оповещения о событиях с применением следующих средств: SMS (short message service); электронных почтовых сообщений; сервиса «v-dial» – автоматического дозвона; звукового (голосового) оповещения.
- Автоматические оповещения о событиях с применением любых интерактивных окон, диалогов и сторонних технических средств.
- Централизованное администрирование компонентов системы, прав и полномочий пользователей.
- Возможность самостоятельного создания любых сценариев работы системы безопасности с помощью макрокоманд, макрособытий и скриптов.
- Глубокая интеграция различных технических средств охраны: ОПС, СКУД, Средства охраны периметра, приборы радиохимического контроля и т.д.
- Синхронное проигрывание видео и аудио информации по одной или нескольким камерам сразу;
- Синхронное проигрывание нескольких потоков;
- Программно реализуемый механизм оптимизации потоков видеoinформации в распределенной цифровой системе видеонаблюдения при недостатке пропускной способности каналов связи;
- Технология GreenStream - автоматический выбор оптимального потока с камеры для снижения нагрузки на процессор и сеть при отображении видео realtime;
- Прямое подключение удаленного рабочего места к камере для отображения realtime видео используется для снижения нагрузки на сеть, в случае если камера транслирует поток в режиме multicast;
- Возможность создания не ограниченного количества раскладок видео камер и других пользовательских интерфейсов;
- Возможность для постоянной и тревожной записей использовать различные потоки с камеры;
- Возможность рекомпрессии видеопотоков в MotionWavelet.
- Поддержка ONVIF профайлы G и S;

- Создание в автоматическом режиме или по расписанию резервных копий видеозаписей на выделенном сервере архива, с возможностью прореживания видеокадров;
- Обработка видеоизображения: цифровое увеличение; контрастирование; фокусировка; маскирование; динамическое оконтуривание.
- Управление поворотными устройствами с возможностью выставять приоритеты различным средствам управления (экранные интерфейсы, клавиатура, джойстик, мышь и так далее);
- Возможность экспортировать видеоархив в фоновом режиме в общедоступные формат (avi) или без изменения формата;
- Присутствие в составе системы портативного проигрывателя видео архива;
- Комплексное использование многозонных детекторов следующих типов: движения, фокусировки, стабильности видеосигнала, изменения фона видеоизображения, засветки объектива видеокамеры, закрытия объектива видеокамеры, детектора оставленных предметов, инфракрасного детектора, детектора лиц;
- Видеоаналитика реального времени на базе технологии «трекер» с заданием условий сработки детекторов и признакам:
  - Детектор настраивается на взаимодействие с любым объектом
  - Детектор срабатывает при любом движении в зоне
  - Детектор срабатывает при входе объекта в зону
  - Детектор срабатывает при выходе объекта из зоны
  - Детектор срабатывает при появлении объекта в зоне
  - Детектор срабатывает при исчезновении объекта в зоне
  - Детектор срабатывает при остановке объекта в зоне
  - Детектор срабатывает при нахождении объекта в зоне более XX сек
  - Детектор срабатывает при оставленном предмете в зоне
  - Детектор срабатывает при пересечении объектом линии в указанном направлении
  - Аналитический поиск по архиву с заданием условий поиска и признакам: тип объекта (любой, машина, человек) и цвет.
  - Будут найдены видеозаписи любого движения в области
  - Будут найдены видеозаписи, в которых осуществляется вход объекта в область
  - Будут найдены видеозаписи, в которых осуществляется выход объекта из области
  - Будут найдены видеозаписи, в которых происходит появление объекта в области
  - Будут найдены видеозаписи, в которых происходит исчезновение объекта в области
  - Будут найдены видеозаписи, в которых объект останавливается в области
  - Будут найдены видеозаписи, на которых объект находится в области более XX секунд
  - Будут найдены видеозаписи, на которых в области имеется оставленный предмет
  - Будут найдены видеозаписи объекта, который пересек линию в указанном направлении
  - Возможность размывать пикселями найденное в кадре лицо.
  - Возможность синхронизации видео архива сервера с внешними хранилищами (карты памяти видеокамер, архивы регистратора и т.д.) - edge storage;
  - Возможность создавать закладки к видеоархиву и потом искать по ним.
  - Возможность проигрывания видеоархива с ускорением, замедлением и в обратном направлении;
  - Другие детекторы: горячие и холодные зоны, подсчет посетителей, подсчет длины очереди, детектор наличия поезда у платформы;
  - Распознавшие автомобильных номеров;
  - Поиск в архиве по номерам;
  - Распознавшие лиц;
  - Поиск в архиве по лицам;

### **3.1.3 ТРЕБОВАНИЯ К БАЗЕ ДАННЫХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

База данных программного обеспечения должна выполнять следующие функции:

- сохранение данных о зарегистрированных системных объектах и параметрах их настройки;
- сохранение данных об учётных записях пользователей и прав пользователей;
- сохранение данных о зарегистрированных в системе событиях;
- сохранение данных об изменениях аппаратно-программной конфигурации;
- сохранение данных об изменениях перечня зарегистрированных системных объектов и параметров их настройки;
- сохранение данных о сетевых именах и IP-адресах компонентов и параметрах взаимодействия между ними;
- репликацию данных, хранящихся на различных компонентах системы;
- синхронизация базы данных серверных компонентов (синхронизация баз данных должна позволять хранить данные как централизованно (на одном серверном компоненте), так и распределено (репликация данных из баз различных серверных компонентов ИСБ)).
- синхронизация баз данных должна обеспечивать параллельную работу с базами данных серверных компонентов и автоматическое обновление при их изменении.

### **3.1.4 ТРЕБОВАНИЯ К ИНТЕГРАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

Интеграция ПО СОВ должна обеспечиваться посредством информационного обмена между программными ядрами. Центральным программным компонентом системы должно являться полнофункциональное программное ядро. С программным ядром системы должны взаимодействовать функциональные модули, являющиеся программной основой функциональных подсистем. Функциональные (программные) модули должны осуществлять непосредственное взаимодействие с аппаратными средствами, а также должны служить источником информации о состоянии подконтрольных объектов. Программное ядро подсистемы должно обрабатывать информацию, поступающую от различных функциональных модулей, и должны обеспечивать их интеграцию.

Исполнительные файлы, соответствующие функциональным подсистемам, должны запускаться ядром автоматически по мере конфигурирования СОВ.

Для упрощения процесса интеграции со смежными информационными системами, дополнительным программным обеспечением или функциональными модулями расширения в программном обеспечении должен быть разработан альтернативный интерфейс информационного обмена функциональных модулей с программным ядром – IIDK (Intellect Integration Developer Kit)/SDK. Должен быть доступен элемент управления ActiveX, являющийся полным аналогом интерфейсного объекта «монитор» и позволяющий управлять камерами, просматривать архив и использовать все функции монитора видеонаблюдения. Должен быть предоставлен программный интерфейс HTTP API, позволяющий отправлять команды и получать данные от СОВ при помощи HTTP-запросов.

### **3.1.5 ТРЕБОВАНИЯ К ИНТЕРАКТИВНОЙ КАРТЕ**

СОВ должна иметь возможность создания интерактивной карты защищаемого объекта. Интерактивная карта должна позволять использовать навигацию между компонентами подсистемы видеонаблюдения с использованием графических планов (схем) подконтрольных территорий. Интерактивная карта должна допускать управление объектами подсистемы из контекстных функциональных меню графических символов

(значков) устройств, размещённых на карте, отображающих (индицирующих) состояние соответствующих системных объектов.

Интерактивная карта должна обладать следующими функциональными возможностями:

- представление объекта на карте в одном из следующих видов:
  - изображение в формате .bmp, .jpg, .png;
  - изображение в формате .bmp, .jpg, .png и индикатор;
  - изображение в формате .svg (векторный формат);
  - текст;
  - линия;
  - многоугольник с количеством вершин до 51;
  - эллипс.
- добавление нескольких значков одного объекта разного вида на один или несколько слоёв интерактивной карты;
- использование набора планов (слоев), представляющих собой фотографии, карты, графические схемы, рисунки в формате bmp., при этом не должны накладываться ограничения на размер и разрешение используемых рисунков;
- задание цвета подложки, в том числе в случае, когда рисунок слоя не выбран;
- при использовании многослойных интерактивных карт – возможность установки правила перехода на слои, содержащие объекты, на которых был зарегистрирован сигнал «Тревога», а также на любые слои, в том числе предыдущий;
- наличие следующих механизмов поиска слоя, с объекта которого поступает тревожный сигнал:
  - вывод окна интерактивной карты поверх всех активных интерфейсных окон при регистрации события «Тревога» на объектах, соответствующих символам, размещённым на слое, с отображением соответствующих слоя и символа;
  - осуществление рекурсивного поиска слоя, с объектов которого поступает тревожный сигнал;
  - подпись к объекту при размещении его на слое карты должна содержать идентификатор объекта после названия или перед ним;
- отключение отображения идентификатора объекта в подписи на карте;
- выбор местоположения подписи относительно значка объекта: сверху, снизу, слева, справа, отсутствует;
- при использовании многослойных интерактивных карт – возможность настраивать механизм перехода с текущего слоя на заданные слои как той же карты, так и других карт в системе (связи со слоем);
- если объект находится в нескольких состояниях, эти состояния должны отображаться на карте посредством последовательной смены изображения или цвета значка объекта;
- при выделении значка объекта справа от него должны отображаться уменьшенные значки всех его состояний;
- отключение отображения уменьшенных значков состояний объектов;
- задание порядка отображения объектов на карте при наложении их изображений друг на друга;
- отображение заданного количества последних событий выбранного объекта в окне Интерактивной карты;

- привязка координат карты к географическим координатам;
- отображение миникарты слоя для упрощения навигации по слою карты.

### 3.1.6 ТРЕБОВАНИЯ К ПРОТОКОЛИРОВАНИЮ СОБЫТИЙ

В подсистеме СОВ должно вестись протоколирование зарегистрированных событий.

Протоколирование должна обладать следующими функциональными возможностями:

- вывод протокола событий на экран в интерфейсном окне;
- выбор в протоколе событий типа объекта, для которого может быть зарегистрировано требуемое событие;
- по умолчанию если ни один тип объекта администратором не задан, то в протокол событий должны записываться все события по всем объектам подсистемы;
- интерфейсное окно протокола событий должно предоставлять возможность просмотра архивных видеозаписей из списка сообщений;
- при выборе объекта в протоколе событий – просмотр данного объекта подсистемы в интерактивной карте защищаемого объекта;
- создание печатной формы отчёта о событиях;
- задание срока хранения архива событий в базе данных протокола событий;
- фильтрация списка событий с использованием заранее настроенных фильтров;
- наличие специализированного протокола событий, предназначенного для оператора, с реализацией следующих функций:
  - отображение в интерфейсном окне событий, зарегистрированных объектами подсистемы;
  - присваивание статуса (типа) зарегистрированному событию (не менее трёх типов);
  - добавление комментария к событию;
  - запись событий в архив;
  - поиск событий в архиве;
  - просмотр видеозаписи события;
  - возможность однократно отложить обработку события на заданный период;
  - эскалация событий в интерфейс вышестоящего лица;
  - генерация событий указанного типа;
  - построение отчётов по фактам обработки событий операторами;
  - построение отчётов по зарегистрированным событиям;
  - определение положения объекта-источника события на карте;
  - подтверждение присвоения типа событию паролём;
  - сортировка событий по приоритету или времени поступления.

### 3.1.7 ТРЕБОВАНИЯ К УДАЛЁННЫМ РАБОЧИМ МЕСТАМ

Клиентское рабочее место должно быть предназначено для использования в качестве рабочих мест операторов и должно реализовывать функции удалённого наблюдения за событиями в системе, контроля состояния тревожных входов, управления исполнительными устройствами и др.

В СОВ должна производиться регистрация следующих категорий пользователей:

- администратор;
- оператор, опционально наделённый правами на администрирование, управление и мониторинг.

Требования к основным интерфейсам рабочих мест (оператора, администрирования):

- древовидная структура расположения объектов (дерево объектов) – многоуровневый вложенный список объектов;
- иерархия объектов – младший в иерархии (дочерний) объект должен быть создан только на базе старшего (родительского объекта);
- возможность отображать дерево объектов в развёрнутом виде, раскрывая и просматривая содержимое всех его групп (ветвей), свёртывать снова, скрывая ненужные для наблюдения в данный момент объекты;
- наличие функции, позволяющей передать ключ активации, регламентирующий конфигурацию системы, на все компьютеры, входящие в систему СОВ;
- поддержка функции создания резервной копии баз данных;
- наличие утилиты, предназначенной для редактирования шаблонов баз данных и файлов внешних настроек;
- наличие утилиты, предназначенной для создания диалоговых окон пользователя;
- наличие утилиты, предназначенной для конвертирования, выбора шаблона и создания резервных копий баз данных;
- наличие утилиты, предназначенной для назначения экранов компьютерам в распределённой системе.

### **3.1.8 ТРЕБОВАНИЯ К СПОСОБАМ И СРЕДСТВАМ СВЯЗИ МЕЖДУ КОМПОНЕНТАМИ СИСТЕМЫ**

Связь между рабочими местами и центральным сервером должна осуществляться по протоколу ТСР/IP с использованием изолированного участка Ethernet-сети, развёрнутой на объекте.

В качестве среды передачи данных должны использоваться провода с медными жилами, оптоволоконные кабели.

Взаимодействие между серверами, УРМА (удалённое рабочее место администрирования), УРММ (удалённое рабочее место мониторинга) должно включать в себя репликацию баз данных (только для серверов и УРМА) и обмен событиями. Настройка взаимодействия компонентов системы должна выполняться с сервера администрирования или, при наличии выделенных подсетей, с узлового сервера или УРМА.

Для каждого компонента СОВ необходимо обеспечить возможность задания списка компонентов, с которыми он осуществляет обмен данными о параметрах конфигурации системы. Для каждого компонента СОВ необходимо обеспечить возможность задания IP-адресов других компонентов СОВ, с которыми требуется осуществлять обмен параметрами конфигурации и событиями.

Для каждого компонента СОВ необходимо обеспечить возможность задания списка компонентов, с которыми он осуществляет обмен событиями.



### **3.1.9 ТРЕБОВАНИЯ К СОВМЕСТИМОСТИ С ДРУГИМИ СИСТЕМАМИ**

В СОВ должна быть предусмотрена интеграция со следующими смежными системами:

- системой СКУД по верхнеуровневому протоколу;
- системой пожарной сигнализации по низкоуровневому протоколу;
- системой охранной сигнализации по низкоуровневому протоколу;

### **3.1.10 ТРЕБОВАНИЯ К РЕЖИМАМ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ**

СОВ должна функционировать в непрерывном круглосуточном режиме (с учетом проведения регламентного технического обслуживания).

### **3.1.11 ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ**

СОВ должна иметь длительный жизненный цикл. Для поддержания соответствия характеристик актуальным требованиям на протяжении всего периода эксплуатации, при разработке СОВ необходимо обеспечить возможность её модернизации в процессе эксплуатации за счёт выбора соответствующей архитектуры программного обеспечения и технических средств, а также за счёт использования стандартизованных и эффективно сопровождаемых решений.

## **3.2 ТРЕБОВАНИЯ К ЧИСЛЕННОСТИ ПЕРСОНАЛА**

Персонал СОВ должен включать следующие категории специалистов:

- пользователи, выполняющие функции администрирования системы;
- операторы системы, выполняющие функции наблюдения и управления системой;
- обслуживающий персонал, обеспечивающий сервисную поддержку работы СОВ.

Администратор должен обладать правами администрирования всех компонентов ИСБ в полном объёме. Оператором должен считаться зарегистрированный в системе пользователь, которому могут быть предоставлены права на администрирование, управление и/или мониторинг отдельных компонентов подсистем.

Регистрация Оператора должна выполняться путём создания учётной записи пользователя и предоставления данному пользователю прав и полномочий на администрирование, управление и/или мониторинг. При регистрации Оператору должен назначаться пароль, используемый для авторизации при запуске и завершении работы программного обеспечения. Дополнительно должна иметься возможность запрета на завершение работы Оператора с программным обеспечением.

Для Администратора не должна создаваться учётная запись, по паролю администратора системы не должна быть выполнена авторизация при запуске программного обеспечения. Пароль Администратора должен использоваться только для получения доступа к диалоговому окну настройки системы, панелям настройки системных объектов, функциям изменения авторизованного пользователя и завершения работы с программным обеспечением.

Учётные записи пользователей должны регистрироваться в программном обеспечении путём создания системных объектов «Пользователь». Для каждого Оператора должна создаваться индивидуальная учётная запись, в которую в дальнейшем должны

добавляться сведения о назначенных правах и заданном для авторизации в программном обеспечении пароле. Должна иметься возможность задавать фамилию, имя и отчество Оператора в различных полях. Полные Ф.И.О. Оператора должны отображаться в дереве системных объектов «Пользователь».

Группа функций администрирования должна включать в себя следующие функции:

- создание и удаление системных объектов;
- редактирование параметров настройки системных объектов;
- перемещения системных объектов по дереву объектов.

По умолчанию Оператору должно быть полностью запрещено использование функций администрирования, но должно быть полностью разрешено использование функций управления и мониторинга на всех объектах, для которых предусмотрены данные функции. Должна иметься возможность запретить Оператору администрирование одного или нескольких объектов, ограничить перечень доступных функций управления объектами, а также ограничить возможности по мониторингу. При предоставлении Оператору прав на администрирование отдельного системного объекта должно выполняться условие — одновременно Оператору предоставляются права на управление и мониторинг по данному объекту.

Право на использование функций управления должно давать возможность использования функциональных интерфейсных кнопок, команд из функциональных меню и прочих средств управления объектами, для которых предусмотрено использование данных функций (дверьми, турникетами, видеокамерами, протоколом событий и т.д.).

В СОВ должна быть предусмотрена возможность смены пароля Оператора в следующих случаях:

- по требованию Оператора;
- по истечении срока действия пароля Оператора;
- при первом входе Оператора в систему.

### **3.3 ПОКАЗАТЕЛИ НАЗНАЧЕНИЯ**

СОВ должна отвечать следующим показателям назначения:

- количество уличных телевизионных камер - 7;
- количество внутренних телевизионных камер - 5;
- глубина видеоархива – 30 сут.;
- глубина отчетов о событиях в базе данных системы: не менее 6 месяцев;
- количество мест оператора системы: не менее 1;
- количество мест администратора системы: не менее 1.

Окончательные значения показателей уточняются в процессе разработки проектной документации и согласовываются протоколом с Заказчиком на стадии разработки рабочей документации.

### **3.4 ТРЕБОВАНИЯ К НАДЕЖНОСТИ**

СОВ должна обеспечивать защиту электрических соединительных цепей от несанкционированных воздействий, приводящих к разблокировке исполнительных устройств.

При размещении оборудования на местах, удовлетворяющих требованиям эксплуатационной документации, СОВ должна обеспечивать необслуживаемое



функционирование в круглосуточном режиме с допустимыми перерывами на профилактику и перенастройку, а также простоями в связи с неисправностью не более 48 часов в год, при среднем времени устранения неисправности, вызвавшей простой, не более 4 часов.

При возникновении сбоев между аппаратной частью и программным обеспечением для сбора и обработки информации система должна продолжать локальное функционирование. В данном случае телевизионные камеры должны продолжать выполнять свои функции в соответствии с алгоритмами, заложенными в их локальной базе данных, а после устранения неисправности телекамера должна передать центральному серверу информацию с внутреннего накопителя, за время отсутствия связи.

При аварийном отключении электропитания СОВ должна переходить на резервный источник электропитания без нарушения функционирования основных компонентов. Расчётное время работы от резервного источника питания должно быть не менее 30 минут.

СОВ должна иметь возможность получать информацию о состояниях основного и резервного источников питания и отображать её на рабочих местах операторов.

СОВ должна иметь возможность исключения вмешательства в логику работы системы со стороны операторов путём разграничения прав доступа к функционалу системы.

Гарантийный срок для видеокамер должен составлять 60 месяцев. Гарантийный срок на поставляемые комплектно товары устанавливается в соответствии с предоставленными паспортами производителей на данные товары и гарантиями производителей, но не менее 12 месяцев.

В соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2007 г. №152-ФЗ «О персональных данных» помещение, в котором будет установлен центральный сервер с базой данных, должно быть оборудовано системами охранной сигнализации и контроля доступа.

### **3.5 ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ**

При монтаже, наладке, эксплуатации, обслуживании и ремонте технических средств СОВ должны выполняться меры электробезопасности в соответствии с ПУЭ и «Правилами техники безопасности при эксплуатации электроустановок потребителей».

Устанавливаемое оборудование СОВ должна отвечать требованиям пожарной безопасности по ГОСТ 12.2.007.0-75 «Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности».

Устанавливаемое оборудование СОВ должна быть заземлена в соответствии с требованиями ГОСТ Р 50571.22-2000 «Электроустановки зданий. Часть 7. Требования к специальным электроустановкам. Раздел 707. Заземление оборудования обработки информации».

Допустимые уровни электромагнитных полей на рабочих местах должны отвечать требованиям ГОСТ 12.1.006-84 «Система стандартов безопасности труда. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля».

### **3.6 ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ**

Силовое питание всей аппаратуры должно осуществляться централизованно, от сети электроснабжения объекта при отсутствии источников импульсных помех от других потребителей.

Средства СОВ должны работать от однофазной промышленной сети переменного тока напряжением 220В, 50Гц по I категории надёжности электроснабжения. Допускается осуществлять электропитания средств СОВ по III категории надёжности электроснабжения.

В данном случае резервное питание средств СОВ должно осуществляться от независимого автономного источника питания с резервированием от аккумуляторных батарей.

Должны обеспечиваться следующие требования к обслуживанию и ремонту СОВ:

- блоки, модули устанавливаемого оборудования должны быть взаимозаменяемыми с аналогичными блоками из ЗИП (холодного резерва) с минимальной настройкой;
- должна быть предусмотрена возможность оперативного ремонта путем замены отказавших узлов и устройств на аналогичные из ЗИП;
- оборудование должно быть размещено таким образом, чтобы обеспечить легкую доступность для проведения оперативного ремонта и замены.

#### 4 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

Стадии разработки и этапы работ, соответствующие ГОСТ 34.601-90, сроки их выполнения, перечень организаций-исполнителей работ, ответственных за проведение работ по этапам и перечень документов по ГОСТ 34.201-89, предъявляемых после окончания соответствующих стадий и этапов работ, приведены в таблице 1.

Таблица 1

Этап работ	Продолжит. этапа, р.д.	Организации исполнители работ	Ответственный за проведение работ	Документы, предъявляемые по окончании этапа
Разработка и утверждение технического задания на проектирование.	2	АО «ПСК» <подрядчик>		Техническое задание на проектирование
Разработка рабочей документации	14	<подрядчик>		Комплект рабочей документации
Строительно-монтажные работы	20	<подрядчик>		Акт завершения работ
Пусконаладочные работы	10	<подрядчик>		Акт завершения работ
Проведение предварительных испытаний	3	<подрядчик>		Акт приёмки в опытную эксплуатацию
Проведение опытной эксплуатации	10	АО «ПСК» <подрядчик>		Акт о завершении опытной эксплуатации и допуске к приёмочным испытаниям
Проведение приёмочных	2	АО «ПСК»		Акт о завершении приёмочных

Этап работ	Продолжит. этапа, р.д.	Организации исполнители работ	Ответственный за проведение работ	Документы, предъявляемые по окончанию этапа
испытаний		<подрядчик>		испытаний и допуске в промышленную эксплуатацию. Акт приёма-сдачи работ.

При проведении экспертизы или согласовании технической документации, разрабатываемой Подрядчиком, на последнего возлагается осуществление технического сопровождения, а также внесение изменений в документацию по обоснованным замечаниям.

## 5 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Вся документация должна быть передана как в напечатанном виде, так и на электронном носителе (текстовая часть в формате DOC или PDF, графическая часть в формате PDF).

Перечень разрабатываемых Подрядчиком комплектов и видов документов на СОВ в целом приведён в таблице 2.

Таблица 2

Стадия (этап) модернизации СОВ	Предъявляемые документы	Кол-во экземпляров
Техническое задание на проектирование	Техническое задание на проектирование	
Рабочая документация	Комплект рабочей документации в составе: <ul style="list-style-type: none"> <li>– Пояснительная записка;</li> <li>– Основной комплект рабочих чертежей (общие данные, структурная схема, планы с прокладкой кабельных трасс, принципиальная схема, кабельный журнал);</li> <li>– Прилагаемая документация (спецификация оборудования и материалов, задания на подключение электропитания 220 В, таблицы для начального конфигурирования приборов и устройств СОВ).</li> </ul>	2+1

## 6 ИСТОЧНИКИ РАЗРАБОТКИ

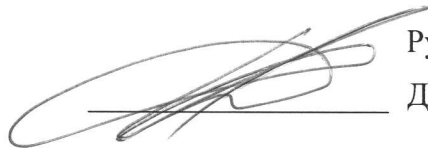
Модернизация СОВ должна выполняться с учётом следующих документов:

- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные»;
- Р 78.36.002-2010 «Выбор и применение систем охранных телевизионных»;
- СП 132.13330.2011 «Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования»;
- ГОСТ Р 21.101-2020 «Система проектной документации для строительства. Основные требования к проектной и рабочей документации» совместно с Поправкой от 08.12.2023;
- Федеральный закон от 22 июля 2008 г. №123-ФЗ "Технический регламент о требованиях пожарной безопасности".
- Постановление Правительства РФ от 16.09.2020 N 1479 "Об утверждении Правил противопожарного режима в Российской Федерации".

## 7 ОСОБЫЕ УСЛОВИЯ

Задание Заказчика может изменяться и дополняться по согласованию сторон.

От Заказчика



Руководитель направления по ИТСО

Д.В. Артемьев

От Подрядчика

---